



PCT/ER 03 / 0 2 8 3 7

Rec'd PCT/ER 03 / 0 2 8 3 7

85 MAR 2005

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 19 DEC 2003

WIPO

PCT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

BEST AVAILABLE COPY

Fait à Paris, le 05 DEC. 2003

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

MISE DES PIÈCES 26 SEP. 2002 0211944 26 SEP. 2002 VP/GEM1326		NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET MARTINET & LAPOUX 43 Boulevard Vauban BP 405 GUYANCOURT 78055 ST QUENTIN YVELINES CEDEX
---------------------------------------------------------------------------------	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE Demande de brevet <input checked="" type="checkbox"/> Demande de certificat d'utilité <input type="checkbox"/> Demande divisionnaire <input type="checkbox"/> Demande de brevet initiale N° / / ou demande de certificat d'utilité initiale N° / / Transformation d'une demande de brevet européen Demande de brevet initiale N° / /	Cochez l'une des 4 cases suivantes

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Identification d'un terminal auprès d'un serveur

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date / / N° Pays ou organisation Date / / N° Pays ou organisation Date / / N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»
5 DEMANDEUR Nom ou dénomination sociale Prénoms Forme juridique N° SIREN Code APE-NAF Adresse Rue Code postal et ville Pays Nationalité N° de téléphone (facultatif) N° de télécopie (facultatif) Adresse électronique (facultatif)		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite» GEMPLUS Société Anonyme 349 711 200 Avenue du Pic de Bertagne Parc d'activité du Gemenos 13420 GEMENOS FRANCE Française



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

REMISE DES PIÈCES		Réservé à l'INPI
DATE	26 SEP. 2002	
LIEU	09	0211944
N° D'ENREGISTREMENT		
NATIONAL ATTRIBUÉ PAR L'INPI		

DB 540 W / 260899

Vos références pour ce dossier : (facultatif)		VP/GEM1326	
6 MANDATAIRE			
Nom		LAPOUX	
Prénom		Roland	
Cabinet ou Société		Cabinet MARTINET & LAPOUX	
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	43 Boulevard Vauban BP 405 GUYANCOURT	
	Code postal et ville	78055 ST QUENTIN YVELINES CEDEX	
N° de téléphone (facultatif)		01.30.64.90.09	
N° de télécopie (facultatif)		01.30.64.90.02	
Adresse électronique (facultatif)		Martinet@wanadoo.fr	
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)		VISA DE LA PRÉFECTURE OU DE L'INPI	
Roland LAPOUX Mandataire (CPI-92-1136)			

Identification d'un terminal auprès d'un serveur

La présente invention concerne l'identification d'un terminal d'utilisateur, et plus particulièrement d'un objet électronique portable personnel à un usager, tel qu'une carte à puce, ou bien d'un usager du terminal auprès d'un serveur. L'identification sert à accéder par l'intermédiaire d'un réseau de télécommunications à un service dispensé par le moyen serveur, tel que l'établissement d'une communication avec un autre terminal d'utilisateur.

Il est connu qu'un usager possédant un terminal radiotéléphonique doit s'identifier auprès d'un serveur dans un réseau de télécommunications quelconque afin d'accéder à un service. Pour cela, un identificateur identifiant le terminal ou l'utilisateur est transmis au moins une fois en clair depuis le terminal au serveur. Puis dans les messages échangés entre le terminal et le serveur, l'identificateur est également présent. Ceci permet à l'administrateur du serveur de gérer le service proposé en fonction des données liées à l'abonnement de l'utilisateur et de gérer la facturation du service.

Dans un tel système terminal-client/serveur, un attaquant peut détecter l'identificateur du terminal ou de l'utilisateur dans les messages transmis par le terminal afin de localiser celui-ci et par exemple d'intercepter et d'horodater les messages transmis depuis le terminal au serveur.

Dans un réseau de radiotéléphonie cellulaire du type GSM, chaque terminal mobile est identifié par un identificateur international unique IMSI (International Mobile Subscriber Identity). Pour des

raisons de sécurité, l'identificateur IMSI est transmis à travers l'interface radio entre le terminal mobile de l'utilisateur et le réseau fixe du réseau de radiotéléphonie que très rarement, par exemple après une mise sous tension du terminal ou après une perte de couverture radioélectrique du terminal. Afin de ménager la confidentialité de l'identificateur de l'utilisateur IMSI, un identificateur temporaire TMSI (Temporary Mobile Subscriber Identity) remplace l'identificateur IMSI chaque fois que le terminal mobile doit s'identifier auprès du réseau fixe du réseau de radiotéléphonie. L'identificateur temporaire TMSI est transmis par l'enregistreur de localisation des visiteurs (VLR) auquel est rattaché momentanément le terminal mobile à chaque mise sous tension du terminal mobile, ou le cas échéant lors d'un changement d'enregistreur VLR pour un transfert du terminal entre des zones de localisation.

Toutefois, lors de certains échanges entre le terminal mobile et l'enregistreur VLR, après une première mise sous tension du terminal, l'identificateur unique IMSI peut être intercepté. La transmission ultérieure de l'identificateur temporaire TMSI ne remédie pas à la substitution de l'identificateur IMSI à l'utilisateur par un attaquant fraudeur.

En outre, le changement de l'identificateur temporaire est décidé par le réseau fixe du réseau de radiotéléphonie, et d'une manière générale par le moyen serveur dans le réseau fixe contenant l'enregistreur VLR, ce qui interdit toute maîtrise de la gestion de son identificateur personnel par l'utilisateur au niveau du terminal mobile.

L'objectif de l'invention est de pallier ces inconvénients afin de ne pas transmettre l'identificateur personnel du terminal ou de l'utilisateur en clair au serveur pendant une session entre le terminal et le serveur, y compris lors de l'établissement de celle-ci, et plus généralement chaque fois que l'identificateur devait être transmis selon la technique antérieure, tout en permettant une identification du terminal ou de l'utilisateur auprès du serveur, ainsi qu'une gestion d'un identificateur réellement transmis au niveau du terminal.

A cette fin, un procédé pour identifier un moyen terminal d'utilisateur ou un utilisateur du moyen terminal par un moyen serveur à travers un réseau de télécommunications, à l'aide d'un premier identificateur, un algorithme asymétrique à clé publique étant implémenté dans le moyen terminal, est caractérisé par :

- une génération d'un nombre aléatoire dans le moyen terminal d'utilisateur,
- une détermination dans le moyen terminal d'un deuxième identificateur en fonction du nombre aléatoire, au moins d'une partie du premier identificateur et du résultat de l'exécution de l'algorithme asymétrique auquel au moins le nombre aléatoire est appliqué,
- une transmission du deuxième identificateur au moyen serveur, et
- dans le moyen serveur, une récupération du premier identificateur au moins par exécution de l'algorithme asymétrique auquel une clé privée et au moins partiellement le deuxième identificateur sont appliqués, afin que le moyen serveur vérifie que le

premier identificateur récupéré soit écrit dans une mémoire du moyen serveur.

Lorsqu'au moins une authentification du moyen terminal par le moyen serveur, ou une
5 authentification mutuelle de ceux-ci, est prévue, les étapes énoncées ci-dessus du procédé de l'invention précédent l'authentification.

Grâce à la détermination d'un deuxième identificateur et à la transmission de celui-ci au
10 moyen serveur, le premier identificateur personnel à l'utilisateur du moyen terminal n'est jamais transmis par le moyen terminal au moyen serveur. Par conséquent, le premier identificateur peut être tout ou partie de l'identificateur d'utilisateur IMSI pour un terminal
15 mobile dans un réseau de radiotéléphonie cellulaire du type GSM demeure protégé dans le moyen terminal. Le deuxième identificateur peut être transmis par le moyen terminal dès le début d'une communication, c'est-à-dire lors de l'établissement d'un appel ou
20 lors de l'établissement d'une session, au moyen serveur afin que le serveur décrypte le deuxième identificateur en le premier identificateur de l'utilisateur et ainsi identifie l'utilisateur.

Tout changement du deuxième identificateur est
25 produit par une génération d'un autre nombre aléatoire dans le moyen terminal. Le moyen terminal gère ainsi localement les changements du deuxième identificateur, indépendamment du moyen serveur, en fonction d'événements particuliers, ou
30 périodiquement, ou bien encore manuellement à la demande de l'utilisateur.

Afin d'augmenter encore la sécurité du premier identificateur de l'utilisateur, la clé publique
nécessaire à l'exécution de l'algorithme asymétrique
35 dans le moyen terminal afin de produire le deuxième

identificateur à transmettre, peut être modifiée au gré du moyen serveur, de préférence après une authentification préalable du moyen serveur par le moyen terminal. Dans ce cas, le procédé
5 d'identification selon l'invention peut comprendre un changement de clé publique et de clé privée pour l'algorithme asymétrique dans le moyen serveur et un téléchargement de la clé publique changée depuis le moyen serveur dans le moyen terminal.

10

L'invention concerne également un moyen terminal d'usager, principalement une carte à puce, s'identifiant ou identifiant un usager de celui-ci auprès d'un moyen serveur, pour la mise en œuvre du
15 procédé d'identification selon l'invention. Le moyen terminal est caractérisé en ce qu'il comprend :

- un moyen pour générer un nombre aléatoire, et
- un moyen pour déterminer un deuxième identificateur en fonction du nombre aléatoire
20 généré, au moins d'une partie du premier identificateur et du résultat de l'exécution de l'algorithme asymétrique auquel au moins le nombre aléatoire est appliqué,

- afin de transmettre le deuxième identificateur
25 au moyen serveur qui récupère le premier identificateur au moins par exécution de l'algorithme asymétrique auquel une clé privée et au moins partiellement le deuxième identificateur sont appliqués et qui vérifie que le premier
30 identificateur récupéré soit écrit dans une mémoire du moyen serveur.

Par exemple, le moyen pour générer un nombre aléatoire et le moyen pour déterminer un deuxième identificateur sont inclus dans un objet électronique
35 portable du type carte à puce.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence
5 aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique d'un réseau de radiotéléphonie cellulaire numérique selon un premier exemple pour la mise en œuvre du procédé de l'invention, dans lequel le moyen terminal
10 est constitué essentiellement par un module d'identité du type carte SIM ;

- la figure 2 montre des étapes du procédé d'identification selon une première réalisation de l'invention qui fait appel à un algorithme
15 asymétrique et un algorithme symétrique ;

- la figure 3 montre des étapes du procédé d'identification selon une deuxième réalisation de l'invention qui fait appel seulement à un algorithme
20 asymétrique ; et

- la figure 4 est un bloc-diagramme schématique d'un réseau de télécommunications entre un terminal du type ordinateur personnel et un serveur selon un deuxième exemple pour la mise en œuvre du procédé
25 selon l'invention.

Selon un premier exemple d'architecture client/serveur de l'invention montré à la figure 1, le moyen terminal d'utilisateur est constitué par un
30 terminal radiotéléphonique mobile d'utilisateur TU, et plus particulièrement par un module amovible, appelé carte SIM (Subscriber Identity Module), du type carte à puce CP, dite également carte à microcontrôleur, inclus dans le terminal TU.

Le terminal radiotéléphonique d'utilisateur TU est
situé à un instant donné dans une zone de
localisation d'un réseau de radiotéléphonie
cellulaire numérique RR, par exemple de type GSM ou
5 UMTS. La zone de localisation est schématisée dans la
figure 1 par la partie fixe du réseau RR comprenant
un commutateur du service mobile MSC qui est relié
d'une part à travers un contrôleur de station de base
BSC à une station de base BTS connectée par voie
10 radio au terminal radiotéléphonique TU, d'autre part
à un commutateur téléphonique à autonomie
d'acheminement du réseau téléphonique commuté RTC.

Le moyen serveur MS selon un premier exemple
d'architecture client/serveur de l'invention regroupe
15 globalement des entités de la partie fixe du réseau
de radiotéléphonie RR servant à la gestion de
l'itinérance des terminaux mobiles, de la sécurité
des communications avec les terminaux mobiles et des
appels entrants et sortants avec les terminaux
20 mobiles dans le réseau RR. Ces entités dans le moyen
serveur MS sont principalement un enregistreur de
localisation des visiteurs VLR relié au moins au
commutateur MSC et contenant des caractéristiques,
telles qu'identités et profils d'abonnement des
25 terminaux mobiles, et plus précisément des usagers
possédant les cartes à puce CP dans ceux-ci, situés
dans la zone de localisation, et un enregistreur de
localisation nominal HLR relié à plusieurs
commutateurs du service mobile MSC à travers le
30 réseau de signalisation du réseau de radiotéléphonie
RR.

Comme on le verra dans la suite, l'enregistreur
VLR n'attribue plus une identité temporaire TMSI pour
identifier chaque terminal mobile TU dans la zone de
35 localisation, mais est transparent à un

identificateur anonyme respectif, comme un pseudonyme IA1, IA2, transmis par chaque terminal d'utilisateur TU pour s'identifier auprès du moyen serveur MS, selon l'invention. Les communications pour les terminaux
5 radiotéléphoniques mobiles visiteurs, tel que le terminal TU montré à la figure 1, se trouvant momentanément dans la zone de localisation desservie par le commutateur MSC sont gérées par celui-ci.

L'enregistreur de localisation nominal HLR est
10 essentiellement une base de données, comme l'enregistreur VLR, qui contient pour chaque terminal mobile TU et plus précisément pour chaque carte SIM CP, un unique identificateur d'utilisateur ID attribué lors de l'abonnement de l'utilisateur au service de
15 radiotéléphonie, en écrivant l'identificateur ID en mémoire non volatile EEPROM de la carte CP. L'identificateur ID identifie également la carte à puce CP et peut être au moins en partie identique à l'identité internationale IMSI notamment pour un
20 réseau de radiotéléphonie du type GSM. L'enregistreur HLR enregistre d'autres caractéristiques liées aux usagers, telles que leurs numéros téléphoniques d'annuaire, leurs profils d'abonnement, etc.

Comme il est connu, l'enregistreur de
25 localisation nominal HLR coopère avec un centre d'authentification AUC bien souvent sur la même plate-forme que l'enregistreur HLR. Le centre d'authentification assure l'authentification des usagers et participe à la confidentialité des données
30 transitant dans les interfaces radio entre les terminaux mobiles TU et les stations de base BTS en gérant des algorithmes d'authentification et de détermination de clé. Le centre d'authentification génère ainsi des clés secrètes d'authentification et
35 des clés de chiffrement respectivement attribuées aux

usagers. En particulier, selon l'invention, le centre d'authentification AUC gère un algorithme asymétrique AA dont la clé privée KPR est mémorisée dans le centre AUC et l'enregistreur HLR, et un algorithme symétrique AS dont la clé dépend d'un nombre aléatoire R selon une première réalisation de l'invention, ou gère seulement un algorithme asymétrique AA à clé privée KPR. Par exemple, l'algorithme asymétrique à clé publique AA peut être l'algorithme de El Gamal, ou de Cramer-Shoup, ou RSA-OAEP (Rivest, Shamir et Adleman-Optimal Asymmetric encryption Padding). En variante, la clé privée KPR n'est pas commune à tous les usagers du réseau RR, mais plusieurs clés privées KPR sont respectivement attribuées à des groupes d'utilisateur en correspondance avec des groupes d'identificateurs d'utilisateur ID, ces correspondances étant enregistrées dans l'enregistreur HLR.

Comme il est connu, la carte à microcontrôleur SIM CP comprend principalement un microprocesseur PR et trois mémoires M1, M2 et M3.

Selon l'invention, un générateur de nombres aléatoires GA est implémenté matériellement dans ou en liaison avec le processeur PR de la carte à puce. Le générateur GA génère un nombre aléatoire R participant à l'identification anonyme de la carte à puce CP en réponse à une requête de la mémoire M1. En variante, le générateur de nombres aléatoires est inclus sous forme de logiciel dans la mémoire ROM M1.

La mémoire M1 est du type ROM et inclut le système d'exploitation de la carte et bien souvent une machine virtuelle sur lequel s'appuie le système d'exploitation. Des algorithmes d'authentification, de communication et d'application, et particulièrement des algorithmes AA et AS, ou AS

selon l'invention sont implémentés dans la mémoire M1. La mémoire M2 est une mémoire non volatile de type EEPROM contenant des caractéristiques liées à l'utilisateur telles que l'identificateur ID de l'utilisateur possédant la carte CP, le profil d'abonnement, un répertoire de numéros téléphoniques, un code confidentiel, etc. La mémoire M2 contient également une clé publique KPU pour l'algorithme asymétrique AA implémenté dans la mémoire M1, associée à la clé privée KPR par l'enregistreur HLR dans le moyen serveur MS, et en variante également en correspondance avec les identificateurs ID des utilisateurs d'un groupe respectif. La mémoire M3 est une mémoire RAM servant au traitement des données à échanger entre le processeur PR et le microcontrôleur inclus dans le terminal mobile TU.

Les deux réalisations du procédé d'identification d'un moyen terminal d'utilisateur TU, CP par un moyen serveur MS selon l'invention sont décrites ci-après en référence au premier exemple montré à la figure 1.

Le procédé d'identification selon l'invention intervient au début E0 d'une session à établir entre le moyen terminal constitué par au moins la carte à puce SIM CP et le moyen serveur MS à travers le réseau de radiotéléphonie RR, par exemple après la mise sous tension du terminal TU ou lors de tout établissement d'appel sortant dans le terminal TU. Plus généralement, le procédé de l'invention peut intervenir chaque fois que la carte à puce doit transmettre, selon la technique antérieure, son identificateur au réseau fixe. Ainsi le procédé de l'invention peut précéder une authentification au

moins de la carte à puce CP par l'enregistreur HLR et le centre d'authentification AUC.

Selon la première réalisation du procédé d'authentification montré à la figure 2, des étapes E1 à E6 succédant à l'étape initiale E0 pour déterminer un identificateur anonyme IA1 sont essentiellement exécutées dans la carte à puce CP, et des étapes E6 à E15 pour récupérer l'identificateur d'utilisateur ID sont exécutées dans le moyen serveur MS du réseau de radiotéléphonie RR.

A l'étape E1, le générateur de nombres aléatoires GA dans la carte à puce CP fournit un nombre aléatoire R qui est mémorisé dans la mémoire M3 pour être appliqué à l'algorithme asymétrique AA et en tant que clé à l'algorithme symétrique AS, implémentés dans la mémoire M1.

La clé publique KPU et l'identificateur d'utilisateur ID sont lus dans la mémoire M2 à des étapes quasi-simultanées E2 et E3 pour être appliqués respectivement aux algorithmes AA et AS. L'application du nombre aléatoire généré R en tant que données à l'algorithme asymétrique AA avec la clé publique KPU produit un nombre aléatoire crypté RC à l'étape E4. En parallèle avec l'étape précédente E4, l'application du nombre aléatoire généré R, en tant que clé secrète unique, et de l'identificateur ID de l'utilisateur, en tant que données, à l'algorithme symétrique AS produit un identificateur crypté IC à l'étape E5. En pratique, une partie de l'identificateur ID est appliquée à l'algorithme AS. Cette partie ne comprend que le numéro confidentiel MSIN (Mobile Subscriber Identification Number) de l'utilisateur inclus dans l'identificateur IMSI de l'utilisateur et identifiant l'utilisateur dans le réseau RR.

Puis après l'exécution des algorithmes AA et AS, le processeur PR concatène le nombre aléatoire crypté RC et l'identificateur crypté IC en un identificateur anonyme IA1 qui est écrit dans la mémoire M2.

5 L'identificateur IA1 constitue un pseudonyme de l'utilisateur, c'est-à-dire de la carte SIM CP en tant que client du moyen serveur MS. Cette concaténation est suivie d'une transmission du pseudonyme IA1 dans un message à travers le terminal TU et le réseau de

10 radiotéléphonie RR vers le moyen serveur MS à l'étape E6. Le pseudonyme IA1 peut être transmis avec les préfixes MCC (Mobile Country Code) et MNC (Mobile Network Code) de l'identificateur IMSI de l'utilisateur afin que l'enregistreur HLR reconnaisse l'indicatif

15 du pays de l'utilisateur et l'indicatif du réseau RR.

Dans le moyen serveur MS, l'enregistreur VLR retransmet l'identificateur anonyme IA1 à l'enregistreur HLR qui, en coopération avec le centre d'authentification AUC, exécute les étapes suivantes

20 E7 à E13.

Après une écriture du nombre aléatoire RC et de l'identificateur IC composant l'identificateur anonyme reçu IA1 dans l'enregistreur HLR à l'étape E7, le centre d'authentification AUC lit la clé privée KPR à l'étape E8 afin de l'appliquer avec le

25 nombre aléatoire crypté reçu RC à l'algorithme asymétrique AA à l'étape E9. Le centre d'authentification AUC récupère ainsi le nombre aléatoire généré R constituant le résultat de

30 l'exécution de l'algorithme AA et l'applique en tant que clé à l'algorithme symétrique AS qui reçoit en tant que données l'identificateur crypté reçu IC lu dans l'enregistreur HLR à l'étape E10.

L'identificateur d'utilisateur ID initialement

35 appliqué à l'étape E5 dans la carte CP est alors

récupéré en sortie de l'algorithme symétrique AS par
 l'enregistreur HLR pour que celui-ci vérifie s'il est
 écrit dans sa base de données à l'étape E11. Si
 l'identificateur récupéré ID n'est pas reconnu, la
 5 session demandée, en l'occurrence un appel, est
 refusée à l'étape E12. Dans le cas contraire,
 l'enregistreur HLR poursuit la session à l'étape E13
 en le signalant à l'enregistreur VLR qui commande
 l'authentification de la carte à puce CP par le
 10 couple HLR-AUC ou une authentification mutuelle de
 ces derniers.

Après l'étape E13, la carte à puce CP transmet
 automatiquement le pseudonyme IA1 lu dans la mémoire
 M2 au moyen serveur MS chaque fois que la carte à
 15 puce doit s'identifier à celui-ci. Cependant, à tout
 moment, comme indiqué à une étape E14, la carte à
 puce CP peut décider de changer de pseudonyme IA1 en
 sollicitant à nouveau le générateur de nombres
 aléatoires GA afin qu'il génère un autre nombre
 20 aléatoire R, à l'étape E1. La génération d'un autre
 nombre aléatoire R par le générateur GA à l'étape E1
 et donc l'exécution d'un nouveau cycle d'étapes E1 à
 E14 peuvent être périodiques dans le moyen terminal
 afin de périodiquement identifier la carte à puce CP
 25 par le moyen serveur MS en déterminant un autre
 identificateur anonyme IA1. Selon une autre variante,
 la génération d'un autre nombre aléatoire R par le
 générateur GA à l'étape E1 et donc l'exécution d'un
 cycle d'étapes E1 à E14 peuvent intervenir sous le
 30 contrôle ou non de l'utilisateur, à la suite par exemple
 au moins de l'un des événements suivants dans le
 moyen terminal constitué par le terminal TU et la
 carte à puce CP : mise sous tension du terminal TU,
 précédant au moins une authentification de la carte à
 35 puce CP par le couple HLR-AUC et une identification

d'un usager du terminal TU par composition d'un code secret PIN sur le clavier du terminal, établissement d'un appel, établissement d'une session entre le moyen terminal et le moyen serveur, substitution du
5 moyen serveur MS à un autre moyen serveur par exemple lors d'un transfert depuis l'enregistreur VLR vers un autre enregistreur VLR du réseau RR auquel est rattaché maintenant le terminal TU, activation d'une application de service telle que l'envoi d'un message
10 court ou d'une connexion à un portail WAP (Wireless Application Protocol) pour terminaux mobiles pour communiquer avec un serveur de site web.

Afin d'améliorer la sécurité de l'identification, l'enregistreur HLR, ou plus
15 généralement le moyen serveur MS, peut décider à tout instant de changer la clé privée actuelle KPR en une autre clé privée et en conséquence la clé publique actuelle KPU en une autre clé publique comme indiqué à une étape E15. Dans ce cas, de préférence après une
20 authentification de l'enregistreur VLR par la carte CP, l'enregistreur HLR commande le téléchargement de l'autre clé publique KPU à travers l'enregistreur VLR, le réseau de radiotéléphonie RR et le terminal TU, dans la mémoire M2 de la carte à puce CP afin que
25 ladite autre clé publique KPU soit utilisée pour les prochaines exécutions de l'algorithme asymétrique AA à l'étape E4. L'autre clé publique KPU est transmise dans un message sécurisé par l'enregistreur VLR au moyen de l'exécution d'un algorithme par exemple
30 symétrique dont la clé secrète a été initialement enregistrée dans la mémoire M2 de la carte à puce CP afin d'authentifier ladite autre clé publique KPU dans le processeur PR.

Selon une deuxième réalisation montrée à la figure 3, au début E0 d'une session à établir entre la carte à puce CP dans le terminal TU et le moyen serveur MS, comme décrit précédemment, le procédé comprend d'abord des étapes E21 à E26 essentiellement exécutées dans la carte SIM CP, puis des étapes E27 à E33 dans le moyen serveur MS. Pour cette deuxième réalisation, la mémoire ROM M1 et le centre d'authentification AUC ne comprennent qu'un algorithme asymétrique à clé publique AA.

A la suite de l'étape E0, le générateur de nombres aléatoires GA génère un nombre aléatoire R qui est écrit dans la mémoire M3 à l'étape E21. L'identificateur ID de la carte à puce CP est lu dans la mémoire M2 à l'étape E22 afin que le processeur PR concatène le nombre aléatoire généré R et au moins une partie de l'identificateur lu ID à l'étape E23. La clé publique KPU est lue dans la mémoire M2 à l'étape E24 pour être appliquée avec la combinaison produite [R, ID], en tant que données, à l'algorithme asymétrique AA à l'étape E25. L'algorithme asymétrique AA est alors exécuté à l'étape E25 et produit un identificateur anonyme IA2 qui est écrit dans la mémoire M2 et qui constitue un pseudonyme, c'est-à-dire de la carte SIM CP que possède l'utilisateur, à l'étape E26. L'identificateur anonyme IA2 représentatif de l'identificateur ID crypté est transmis dans un message par la carte à puce CP à travers le terminal TU et le réseau de radiotéléphonie RR vers le moyen serveur MS.

L'enregistreur de localisation des visiteurs VLR retransmet l'identificateur anonyme IA2 à l'enregistreur HLR qui l'écrit en mémoire à l'étape E27. A l'étape E28, la clé privée KPR est lue dans l'enregistreur HLR qui exécute les étapes suivantes

E29 à E33 en coopération avec le centre d'authentification AUC. La clé lue KPR et l'identificateur IA2, en tant que données, sont appliqués à l'algorithme asymétrique AA dans le
5 centre d'authentification AUC, à l'étape E29. L'exécution de l'algorithme AA permet de récupérer le nombre aléatoire R et surtout l'identificateur d'utilisateur ID à l'étape E30.

L'étape E30 est suivie d'étapes E31 à E35 qui
10 sont respectivement analogues aux étapes E11 à E15 et qui concernent la vérification de l'appartenance de l'identificateur récupéré ID à la base de données dans l'enregistreur HLR, la transmission automatique de l'identificateur anonyme IA2 par la carte à puce
15 CP chaque fois que celle-ci doit s'identifier auprès du moyen serveur MS, le changement de préférence automatique d'identificateur anonyme IA2 soit périodiquement soit à la suite de l'un au moins des événements énoncés précédemment, et le téléchargement
20 d'une autre clé publique KPU dans la carte à puce CP à la suite d'un changement de clé privée KPR dans le moyen serveur MS.

Selon une variante des réalisations décrites ci-dessus, l'enregistreur de localisation des visiteurs
25 VLR dans le réseau RR contient les algorithmes AA et AS, qui sont exécutés aux étapes E9 et E10, ou l'algorithme AS qui est exécuté à l'étape E29, au lieu d'être implémentés et exécutés dans le centre
30 d'authentification.

Selon un deuxième exemple d'architecture client/serveur selon l'invention montré à la figure
4, le moyen terminal est un ordinateur personnel PC
35 ou un assistant numérique personnel (PDA) ou tout

autre objet électronique notamment portable qui est
 relié à un réseau de télécommunications RT. Le réseau
 RT peut inclure le réseau internet et un réseau
 d'accès tel que le réseau téléphonique commuté, ou
 5 bien constituer un réseau local, par exemple un
 réseau local sans fil WLAN (Wireless Local Area
 Network). Le terminal PC comprend notamment en
 relation avec l'invention, une mémoire ME de
 préférence sécurisée dans laquelle sont implémentés
 10 les algorithmes AA et AS, ou l'algorithme AA, et sont
 mémorisés l'identificateur d'utilisateur ID et la clé
 publique KPU. Le terminal PC contient un navigateur
 jouant le rôle de client par rapport à un serveur SE,
 en tant que moyen serveur selon l'invention, relié au
 15 réseau de télécommunications RT. Dans le serveur SE
 sont également implémentés les algorithmes AA et AS
 selon la première réalisation, ou l'algorithme AA
 selon la deuxième réalisation, et sont mémorisées la
 clé privée KPR et la clé publique KPU de préférence
 20 en correspondance avec un identificateur ID d'un
 usager du terminal PC, tel que log-in, comme dans le
 moyen serveur MS selon le premier exemple. Dans cet
 exemple, le serveur SE est par exemple un site ou un
 portail web qui gère au moins l'accès à une base de
 25 données à laquelle l'utilisateur du terminal PC est
 abonné.

Des étapes analogues à celles décrites E1 à E15,
 ou E21 à E35 sont exécutées pour partie dans le
 terminal PC et pour partie dans le serveur SE afin
 30 d'identifier un usager du terminal TU par comparaison
 de l'identificateur récupéré ID par le serveur SE et
 l'identificateur d'utilisateur mémorisé dans le serveur.
 Ces étapes peuvent précéder d'autres étapes de
 sécurisation relatives notamment à une

authentification de l'utilisateur par vérification d'un mot de passe de l'utilisateur.

En variante, le terminal PC est doté d'un lecteur pour carte à puce additionnelle CA qui est analogue à la carte à puce CP selon le premier exemple montré à la figure 1, c'est-à-dire dont les mémoires M1 et M2 contiennent des algorithmes AA et AS selon la première réalisation, ou l'algorithme AA selon la deuxième réalisation, l'identificateur ID de l'utilisateur possesseur de la carte CA et donc de la carte CA elle-même et la clé publique KPU. Comme dans l'exemple montré à la figure 1, le terminal PC dans cette variante est transparent aux communications entre le serveur SE et la carte CA en ce qui concerne l'identification de la carte CA par le serveur SE selon l'invention. La liaison entre la carte CA et le terminal PC est classique et peut être une liaison à contact électrique, une liaison dite sans contact, ou une liaison radioélectrique de proximité du type Bluetooth ou 802.11.

Selon encore une autre variante du deuxième exemple montré à la figure 4, la carte à puce CA a seulement mémorisé l'identificateur ID et la clé publique KPU dans sa mémoire EEPROM M2, et les algorithmes AA et AS, ou l'algorithme AA, sont implémentés dans le terminal PC.

Dans ces variantes du deuxième exemple, le terminal PC et la carte à puce additionnelle CA peuvent être respectivement un terminal bancaire et une carte de crédit, ou un terminal point de vente et un porte-monnaie électronique.

REVENDICATIONS

- 1 - Procédé pour identifier un moyen terminal d'utilisateur (TU, CP ; PC, CA) ou un usager du moyen terminal par un moyen serveur (MS ; SE) à travers un réseau de télécommunications (RR ; RT), à l'aide d'un premier identificateur (ID), un algorithme asymétrique (AA) à clé publique (KPU) étant implémenté dans le moyen terminal, caractérisé par :
- 10 - une génération (E1, E21) d'un nombre aléatoire (R) dans le moyen terminal d'utilisateur (TU, CP ; PC, CA),
 - une détermination (E4, E5 ; E25) dans le moyen terminal d'un deuxième identificateur (IA1 ; IA2) en fonction du nombre aléatoire (R), au moins d'une partie du premier identificateur (ID) et du résultat de l'exécution de l'algorithme asymétrique (AA) auquel au moins le nombre aléatoire est appliqué,
 - 20 - une transmission (E6 ; E26) du deuxième identificateur (IA1 ; IA2) au moyen serveur (MS ; SE), et
 - dans le moyen serveur, une récupération (E9, E10 ; E29) du premier identificateur (ID) au moins par exécution de l'algorithme asymétrique (AA) auquel une clé privée (KPR) et au moins partiellement le deuxième identificateur (IA1 ; IA2) sont appliqués,
 - 25 afin que le moyen serveur vérifie que le premier identificateur récupéré (ID) soit écrit dans une mémoire (HLR) du moyen serveur.
- 30
- 2 - Procédé conforme à la revendication 1, dans lequel les étapes énoncées dans la revendication 1 précèdent au moins une authentification (E13) du moyen terminal (TU, CP ; PC, CA) par le moyen serveur
- 35 (MS ; SE).

3 - Procédé conforme à la revendication 1 ou 2,
dans lequel la détermination dans le moyen terminal
(TU, CP ; PC, CA) comprend une application (E4) du
5 nombre aléatoire généré (R) à l'algorithme
asymétrique (AA) avec la clé publique (KPU) pour
produire un nombre aléatoire crypté (RC), une
application (E5) du nombre aléatoire généré (R) en
tant que clé et du premier identificateur (ID) à un
10 algorithme symétrique (AS) implémenté dans le moyen
terminal pour produire un identificateur crypté (IC),
et une concaténation (E6) du nombre aléatoire crypté
(RC) et de l'identificateur crypté (IC) en le
deuxième identificateur (IA1) à transmettre au moyen
15 serveur (MS ; SE), et la récupération dans le moyen
serveur comprend l'application (E9) du nombre
aléatoire crypté (RC) à l'algorithme asymétrique (AA)
avec la clé privée (KPR) pour récupérer le nombre
aléatoire généré (R), et l'application (E10) du
20 nombre aléatoire récupéré (R) en tant que clé et de
l'identificateur crypté (IC) à l'algorithme
symétrique (AS) afin de récupérer le premier
identificateur (ID).

25 4 - Procédé conforme à la revendication 1 ou 2,
selon lequel la détermination dans le moyen terminal
(TU, CP ; PC, CA) comprend l'application (E25) du
nombre aléatoire généré (R) et du premier
identificateur (ID) concaténés à l'algorithme
30 asymétrique (AA) avec la clé publique (KPU) pour
produire le deuxième identificateur (IA2) à
transmettre au moyen serveur (MS ; SE), et la
récupération dans le moyen serveur comprend
l'application (E29) du deuxième identificateur (IA2)
35 à l'algorithme asymétrique (AA) avec la clé privée

(KPR) afin de récupérer le premier identificateur (ID).

5 - Procédé conforme à l'une quelconque des
5 revendications 1 à 4, comprenant un changement (E15 ; E35) de clé publique (KPU) et de clé privée (KPR) pour l'algorithme asymétrique (AA) dans le moyen serveur (MS ; SE) et un téléchargement (E15 ; E35) de la clé publique changée (KPU) depuis le moyen serveur
10 dans le moyen terminal (TU, CP ; PC, CA).

6 - Procédé conforme à l'une quelconque des revendications 1 à 5, selon lequel la génération de nombre aléatoire (E1) est périodique (E14 ; E34) dans
15 le moyen terminal (TU, CP ; PC, CA).

7 - Procédé conforme à l'une quelconque des revendications 1 à 6, selon lequel la génération de nombre aléatoire (E1) intervient (E14 ; E34) à la
20 suite au moins de l'un des événements suivants dans le moyen terminal (TU, CP ; PC, CA) : mise sous tension du moyen terminal, établissement d'un appel, établissement d'une session entre le moyen terminal et le moyen serveur, substitution du moyen serveur à
25 un autre moyen serveur, activation d'une application de service.

8 - Moyen terminal d'utilisateur (TU, CP ; PC, CA) s'identifiant ou identifiant un usager de celui-ci
30 auprès d'un moyen serveur (MS ; SE) à travers un réseau de télécommunications (RR ; RT), à l'aide d'un premier identificateur (ID), un algorithme asymétrique (AA) à clé publique (KPU) étant implémenté dans le moyen terminal, caractérisé en ce
35 qu'il comprend :

- un moyen (GA) pour générer un nombre aléatoire (R), et
- un moyen (PR, M1) pour déterminer un deuxième identificateur (IA1 ; IA2) en fonction du nombre aléatoire, au moins d'une partie du premier identificateur (ID) et du résultat de l'exécution de l'algorithme asymétrique (AA) auquel au moins le nombre aléatoire est appliqué,
- afin de transmettre le deuxième identificateur (IA1 ; IA2) au moyen serveur (MS ; SE) qui récupère le premier identificateur au moins par exécution de l'algorithme asymétrique (AA) auquel une clé privée (KPR) et au moins partiellement le deuxième identificateur (IA1 ; IA2) sont appliqués et qui vérifie que le premier identificateur récupéré (ID) soit écrit dans une mémoire (HLR) du moyen serveur.

9 - Moyen terminal d'utilisateur conforme à la revendication 8, dans lequel le moyen pour générer un nombre aléatoire (GA) et le moyen pour déterminer un deuxième identificateur (PR, M1) sont inclus dans un objet électronique portable du type carte à puce (CP ; CA).

1/3
FIG. 1

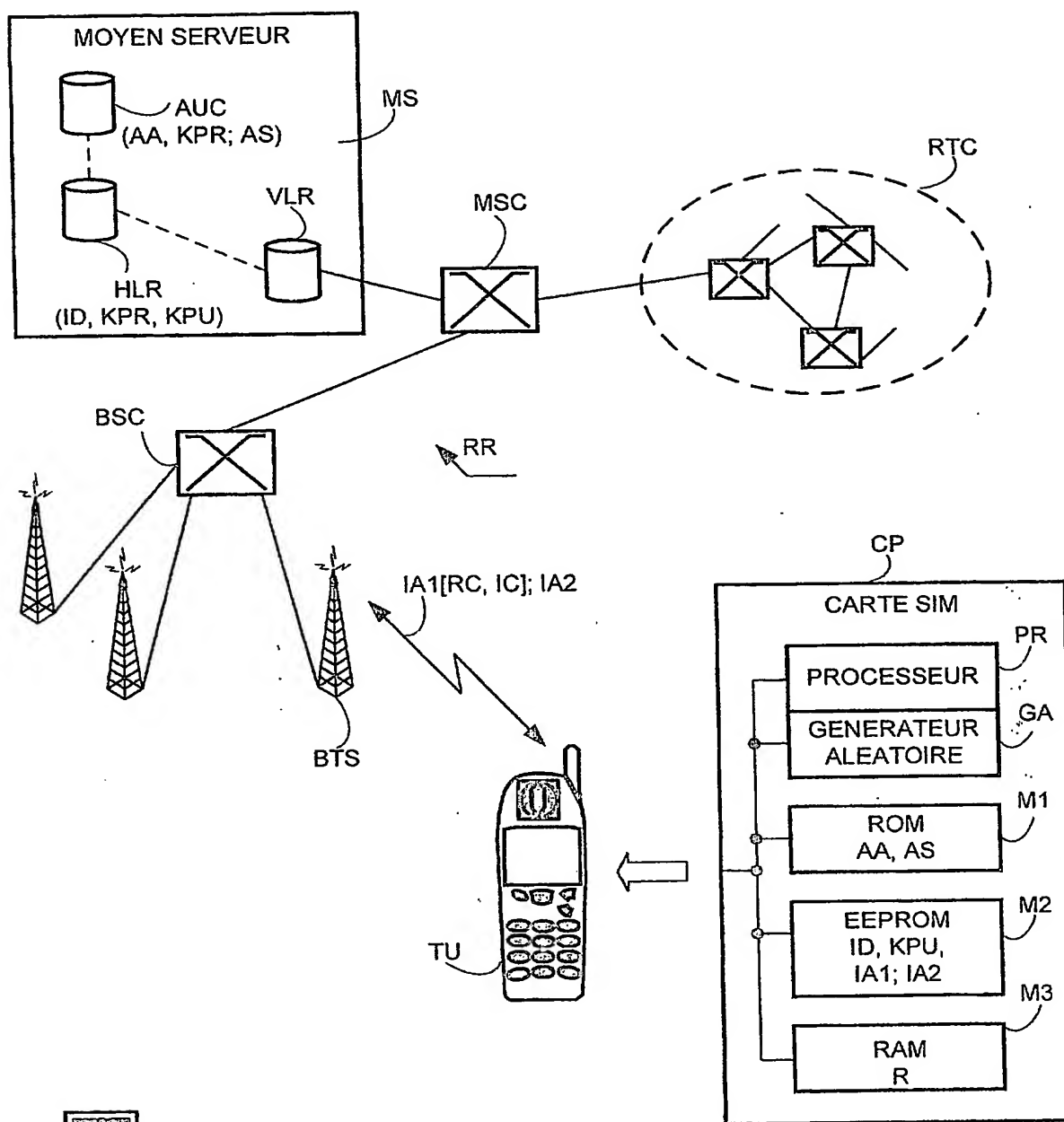
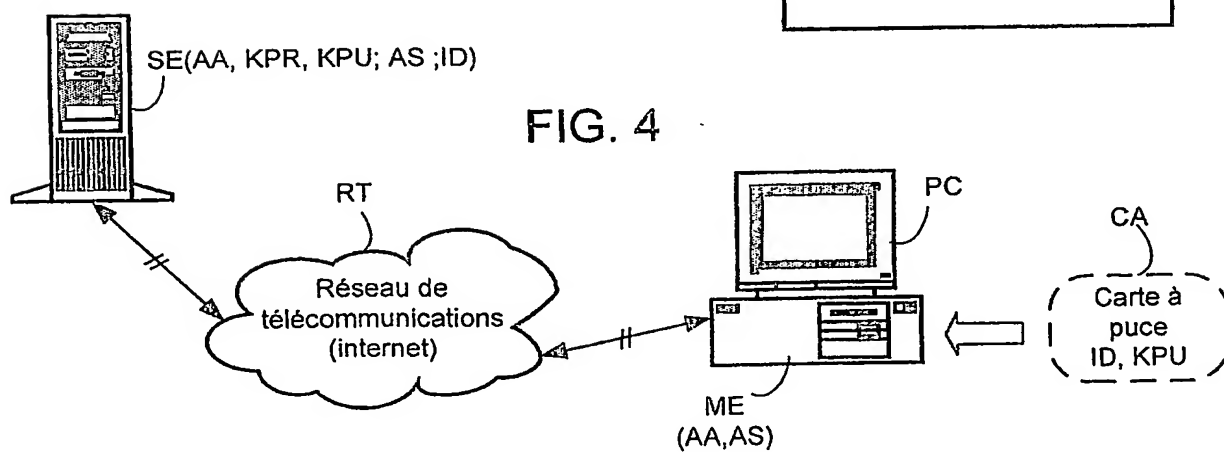


FIG. 4



2/3

FIG. 2

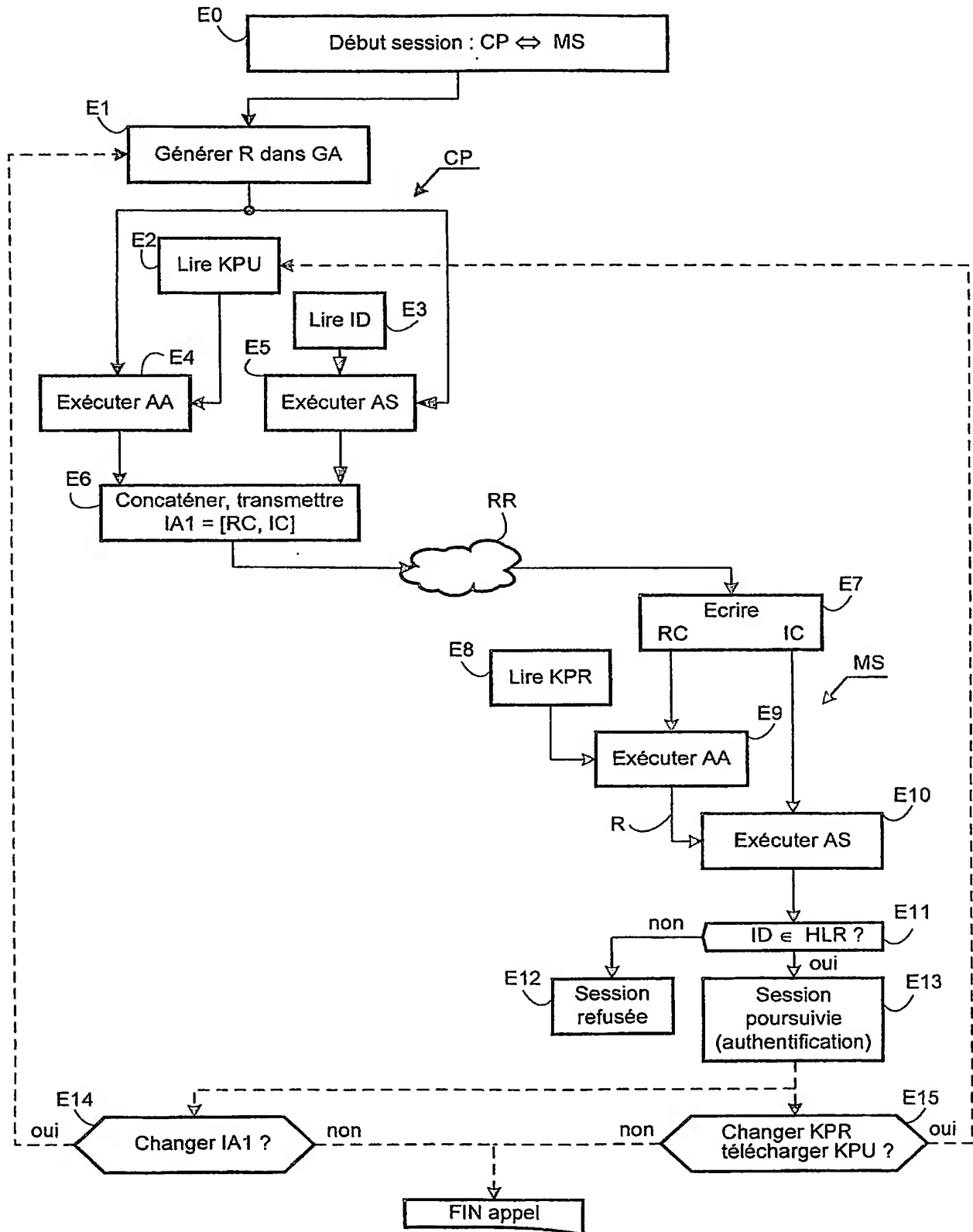
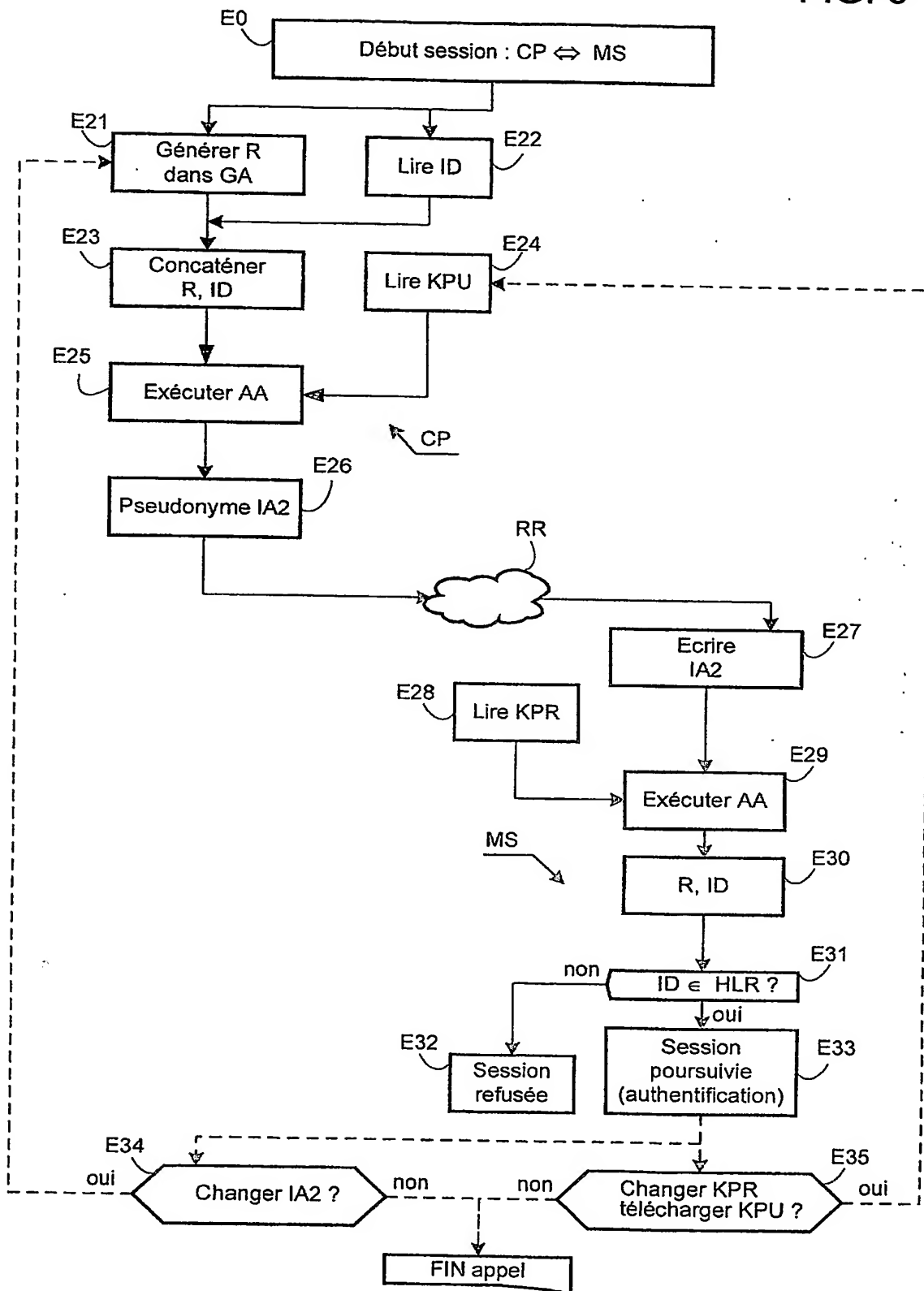


FIG. 3





BREVET D'INVENTION

CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11235*02

ÉPARTEMENT DES BREVETS

6 bis, rue de Saint Pétersbourg

5800 Paris Cedex 08


téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° . 1. / . 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

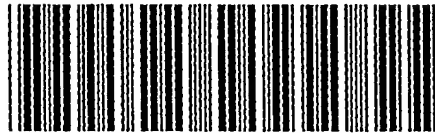
Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		VP/GEM1326	
N° D'ENREGISTREMENT NATIONAL		02/M 564	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Identification d'un terminal auprès d'un serveur			
LE(S) DEMANDEUR(S) :			
GEMPLUS Avenue du Pic de Bertagne Parc d'activité de Gemenos 13420 GEMENOS			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		De GROOT	
Prénoms		Max	
Adresse	Rue	10 Lot. l'Acadie	
	Code postal et ville	13720	LA BOUILLADISSE
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Roland LAPOUX Mandataire (CPI/92-1136) 	
		Le 25 Septembre 2002	

PCT Application

FR0302837



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.